# Glossary

## Symbols

3DES See definition for Triple DES (3DES).

## A

abstract classes Templates used only to derive new Structural classes. Abstract classes cannot be instantiated in the directory.

access control A security mechanism that determines which operations a user, group, service, or computer is authorized to perform on a computer or on a particular object, such as a file, printer, registry subkey, or directory service object. See also group; object; permission; registry.

access control list (ACL) A list of security protections that apply to an entire object, a set of the object's properties, or an individual property of an object. There are two types of access control lists: discretionary and system. See also object.

ACL See definition for access control list (ACL).

Active Directory The Windows-based directory service. Active Directory stores information about objects on a network and makes this information available to users and network administrators. Active Directory gives network users access to permitted resources anywhere on the network using a single logon process. It provides network administrators with an intuitive, hierarchical view of the network and a single point of administration for all network objects. See also directory partition; directory service; domain; forest; object.

Active Directory Service Interfaces (ADSI) A directory service model and a set of Component Object Model (COM) interfaces. ADSI enables Windows applications and Active Directory clients to access several network directory services, including Active Directory. ADSI is supplied as a software development kit (SDK). See also Active Directory; Component Object Model (COM); directory service.

ActiveX A set of technologies that allows software components to interact with one another in a networked environment, regardless of the language in which the components were created.

Address Resolution Protocol (ARP) In TCP/IP, a protocol that uses broadcast traffic on the local network to resolve a logically assigned Internet Protocol version 4 (IPv4) address to its physical hardware or media access control (MAC) layer address.

In asynchronous transfer mode (ATM), ARP is used two different ways. For classical IPv4 over ATM (CLIP), ARP is used to resolve addresses to ATM hardware addresses. For ATM LAN emulation (LANE), ARP is used to resolve Ethernet/802.3 or Token Ring addresses to ATM hardware addresses.

See also asynchronous transfer mode (ATM); Internet Protocol (IP); IP address; packet; Transmission Control Protocol/Internet Protocol (TCP/IP).

administrative credentials Logon information that is used to identify a member of an administrative group. Groups that use administrative credentials include Administrators, Domain Admins, and DNS Admins. Most system-wide or domain-wide tasks require administrative credentials. See also Administrators group; group.

Administrators group On a local computer, a group whose members have the highest level of administrative access to the local computer. Examples of administrative tasks that can be performed by members of this group include installing programs; accessing all files on the computer; auditing access control; and creating, modifying, and deleting local user accounts.

In an Active Directory domain, a group whose members have the highest level of administrative access in the domain. Examples of administrative tasks that can be performed by members of this group include setting domain policy; assigning and resetting domain user account passwords; setting up and managing domain controllers; and creating, modifying, and deleting domain user accounts.

See also access control; Active Directory; auditing; domain; domain controller; group; object.

**ADSI** See definition for Active Directory Service Interfaces (ADSI).

**ADSI provider** COM objects that implement ADSI for a particular namespace (for example, an LDAP namespace such as Active Directory).

**agent** An application that runs on a Simple Network Management Protocol (SNMP) managed device. The agent application is the object of management activities. A computer running SNMP agent software is also sometimes referred to as an agent.

**aggregation** A composition technique for implementing component objects in which a new object can be built by using one or more existing objects that support some or all of the new object's required interfaces.

**American Standard Code for Information Interchange (ASCII)** A standard single-byte character encoding scheme used for text-based data. ASCII uses designated 7-bit or 8-bit number combinations to represent either 128 or 256 possible characters. Standard ASCII uses 7 bits to represent all uppercase and lowercase letters, the numbers 0 through 9, punctuation marks, and special control characters used in U.S. English. Most current x86-based systems support the use of extended (or "high") ASCII. Extended ASCII allows the eighth bit of each character to identify an additional 128 special symbol characters, foreign-language letters, and graphic symbols.

**Anonymous access** An authentication mechanism by which users who are able to connect to an Internet site without credentials are assigned to the IUSR_*ComputerName* account and granted the access rights that are assigned to that account. See also access control; Anonymous authentication; authentication.

**Anonymous authentication** An authentication mechanism that does not require user accounts and passwords. Anonymous authentication grants remote users the identity IUSR_*ComputerName*. Anonymous authentication is used on the Internet to grant visitors restricted access to predefined public resources. See also Anonymous access; authentication.

**Anonymous FTP authentication** A protocol that makes it possible for a user to retrieve documents, files, programs, and other archived data from anywhere on the Internet without having to establish a logon name and password.

**apartment-threaded** A threading model in which each method of a component will execute on a thread that is associated with that component. See also multithreaded apartment (MTA); single-threaded apartment (STA).

**API** See definition for application programming interface (API).

**application** A computer program, such as a word processor or electronic spreadsheet, or a group of Active Server Pages (ASP) scripts and components that perform such tasks.

**application isolation** The separation of applications by process boundaries that prevent the applications from affecting one another. Application isolation is configured differently for each of the two Internet Information Services (IIS) isolation modes. See also IIS 5.0 isolation mode; worker process isolation mode.

**application pool** A grouping of one or more URLs served by a worker process.

**application programming interface (API)** A set of routines that an application uses to request and carry out lower-level services performed by a computer's operating system. These routines usually carry out maintenance tasks such as managing files and displaying information.

**application root** The root directory for an application. All directories and files contained within the application root are considered part of the application. Also called an application starting-point directory.

**application scope** A way of making data available to all users of an application from all pages of a Web application. A variable or an object instance is given application scope by being stored in the Active Server Pages (ASP) application object. Application scope is useful for global data, such as a global counter.

**argument** A constant, variable, or expression that is passed to a procedure.

**array** A list of data values—all of the same type—any element of which can be referenced by an expression that consists of the array name followed by an indexing expression. Arrays are part of the fundamentals of data structures, which, in turn, are a major fundamental of computer programming.

**ASCII (American Standard Code for Information Interchange)** See definition for American Standard Code for Information Interchange (ASCII).

**ASP buffering** Functionality of Active Server Pages (ASP) that temporarily stores all output that is generated by a script until script execution is complete and then sends the output to a client.

**association** In file name extension mapping, the linking of a file extension, such as .asp, to an application, such as asp.dll. In Windows Management Instrumentation (WMI), an association class represents a relationship between two specific WMI classes. The properties of an association class include pointers, or references, to the two classes or instances.

**asymmetric key algorithm** See definition for public-key algorithm.

**asynchronous transfer mode (ATM)** A high-speed, connection-oriented, virtual circuit-based packet switching protocol used to transport many different types of network traffic. ATM packages data in 53-byte, fixed-length cells that can be switched quickly between logical connections on a network. See also protocol.

**ATM** See definition for asynchronous transfer mode (ATM).

**attribute** For files, information that indicates whether a file is read-only, hidden, ready for archiving (backing up), compressed, or encrypted, and whether the file contents should be indexed for fast file searching.

In Active Directory, a property of an object. For each object class, the schema defines which attributes an instance of the class must have and which additional attributes it might have.

See also Active Directory; class; object.

**auditing** The process that tracks the activities of users by recording selected types of events in the security log of a server or a workstation.

**authentication** The process for verifying that an entity or object is who or what it claims to be. Examples include confirming the source and integrity of information, such as verifying a digital signature or verifying the identity of a user or computer. See also cryptography; Kerberos V5 authentication protocol.

**authorization**

The process that determines what a user is permitted to do on a computer system or network. See also authentication.

**Automation** A Component Object Model (COM) based technology that allows for interoperability among ActiveX components, including OLE components. Formerly referred to as *OLE Automation*.

**availability** A level of service provided by applications, services, or systems. Highly available systems have minimal downtime, whether planned or unplanned. Availability is often expressed as the percentage of time that a service or system is available, for example, 99.9 percent for a service that is down for 8.75 hours a year.

# B

**bandwidth** The data transfer capacity of a transmission medium.

In digital communications, the transfer capacity expressed in bits per second (bps) or megabits per second (Mbps). For example, Ethernet accommodates a bandwidth of 10,000,000 bps or 10 Mbps.

In analog communications, the difference between the highest and lowest frequencies in a specific range. For example, an analog telephone line accommodates a bandwidth of 3,000 hertz (Hz), the difference between the lowest (300 Hz) and highest (3,300 Hz) frequencies that it can carry.

See also bits per second (bps).

**bandwidth throttling** Setting the maximum portion of total network capacity that a service is allowed to use. An administrator can deliberately limit a server's Internet workload by not allowing it to receive requests at full capacity, thus saving resources for other programs, such as e-mail.

**baseline** A range of measurements derived from performance monitoring that represents acceptable performance under typical operating conditions.

**Basic authentication** An authentication mechanism that is supported by most browsers, including Internet Explorer. Basic authentication encodes user name and password data before transmitting it over the network. Note that *encoding* is not the same as *encryption*. Also known as *plaintext authentication*. See also Anonymous authentication; authentication; Digest authentication; encryption.

baud rate The speed at which a modem communicates. Baud rate refers to the number of times the condition of the line changes. This is equal to bits per second only if each signal corresponds to one bit of transmitted data.

Modems must operate at the same baud rate in order to communicate with each other. If the baud rate of one modem is set higher than that of the other, the faster modem usually alters its baud rate to match that of the slower modem.

See also bits per second (bps); modem (modulator/demodulator).

Berkeley Internet Name Domain (BIND) An implementation of Domain Name System (DNS) written and ported to most available versions of the UNIX operating system. The Internet Software Consortium maintains the BIND software. See also Domain Name System (DNS).

binary A base-2 number system in which values are expressed as combinations of two digits, 0 and 1.

BIND See definition for Berkeley Internet Name Domain (BIND).

binding A process by which software components and layers are linked together. When a network component is installed, the binding relationships and dependencies for the components are established. Binding allows components to communicate with each other.

bitmask A value that is used with bit-wise operators (And, Eqv, Imp, Not, Or, Xor) to test the state of individual bits in a particular bit-field value. See also bitmask identifier.

bitmask identifier For the metabase, a name assigned to a bitmask to help identify its purpose. For example, In IIS 6.0, bitmask 512 is assigned the identifier MD_ACCESS_SCRIPT. See also bitmask.

bits per second (bps) The number of bits transmitted every second, used as a measure of the speed at which a device, such as a modem, can transfer data. See also modem (modulator/demodulator).

Boolean data type A data type with only two passable values, True (-1) or False (0). Boolean variables are stored as 16-bit (2-byte) numbers.

both-threaded A threading model in which the object has the characteristics of an apartment-threaded object as well as a free-threaded object. See also apartment-threaded.

bps See definition for bits per second (bps).

browser Software that interprets the markup of files in HTML, formats them into Web pages, and displays them to the end user. Some browsers also permit end users to send and receive e-mail, read newsgroups, and play sound or video files embedded in Web documents.

built-in groups The default security groups installed with the operating system. Built-in groups have been granted useful collections of rights and built-in abilities.

In most cases, built-in groups provide all the capabilities needed by a particular user. For example, members of the built-in Backup Operators group can back up and restore files and folders. To provide a needed set of capabilities to a user account, assign it to the appropriate built-in group.

See also group.

bulk encryption A process in which large amounts of data, such as files, e-mail messages, or online communications sessions, are encrypted for confidentiality. It is usually done with a symmetric key algorithm. See also encryption.

## C

CA See definition for certification authority (CA).

cache A special memory subsystem in which frequently used data values are duplicated for quick access.

call To transfer program execution to some section of code (usually a subroutine) while saving the necessary information to allow execution to resume at the calling point when the called section has completed execution. When a subroutine call occurs, one or more values (known as arguments or parameters) are often passed to the subroutine, which can then use and sometimes modify these values.

callback function A function provided by Internet Information Services (IIS) that allows an Internet Server API (ISAPI) extension or filter to access IIS services.

certificate A digital document that is commonly used for authentication and to secure information on open networks. A certificate securely binds a public key to the entity that holds the corresponding private key. Certificates are digitally signed by the issuing certification authority (CA), and they can be issued for a user, a computer, or a service. See also certification authority (CA); private key; public key.

**certificate revocation list (CRL)** A document maintained and published by a certification authority that lists certificates that have been revoked. See also certificate; certification authority (CA).

**certificate trust list (CTL)** A signed list of root certification authority certificates that an administrator considers reputable for designated purposes, such as client authentication or secure e-mail. See also certificate; certification authority (CA).

**certificate, client** See definition for client certificate.

**certification authority (CA)** An entity responsible for establishing and vouching for the authenticity of public keys belonging to subjects (usually users or computers) or other certification authorities. Activities of a certification authority can include binding public keys to distinguished names through signed certificates, managing certificate serial numbers, and certificate revocation. See also certificate; public key.

**CGI** See definition for common gateway interface (CGI).

**class** A category of objects that share a common set of characteristics. Each object in the directory is an instance of one or more classes in the schema. See also object.

**client** Any computer or program connecting to, or requesting the services of, another computer or program. Client can also refer to the software that enables the computer or program to establish the connection.

For a local area network (LAN) or the Internet, a computer that uses shared network resources provided by another computer (called a *server*).

See also server.

**client certificate** A digital certificate that functions in a manner that is similar to a driver's license or passport. Client certificates can contain detailed identification information about the user and organization that issued the certificate.

**client tier** In the three-tier Web application model, the application or process that requests services from the middle tier, which typically includes a Web server and business processes. See also data source tier; middle tier.

**client/server architecture** A model of computing in which client applications running on a desktop or personal computer access information on remote servers or host computers. The client portion of the application is typically optimized for user interaction, whereas the server portion provides centralized, multi-user functionality.

**cluster** In data storage, the smallest amount of disk space that can be allocated to hold a file. All file systems used by Windows organize hard disks based on clusters, which consist of one or more contiguous sectors. The smaller the cluster size, the more efficiently a disk stores information. If no cluster size is specified during formatting, Windows picks defaults based on the size of the volume. These defaults are selected to reduce the amount of space that is lost and the amount of fragmentation on the volume. Also called an *allocation unit*.

In computer networking, a group of independent computers that work together to provide a common set of services and present a single-system image to clients. The use of a cluster enhances the availability of the services and the scalability and manageability of the operating system that provides the services.

See also availability; client; scalability.

**code page** A means of providing support for character sets and keyboard layouts for different countries or regions. A code page is a table that relates the binary character codes used by a program to keys on the keyboard or to characters on the display.

**COM** See definition for Component Object Model (COM).

**COM+** An extension of the COM (Component Object Model) programming architecture that includes a runtime or execution environment and extensible services, including transaction services, security, load balancing, and automatic memory management. See also Component Object Model (COM).

**common gateway interface (CGI)** A server-side interface for initiating software services. For example a set of interfaces that describe how a Web server communicates with software on the same computer. Any software can be a CGI program if it handles input and output according to the CGI standard.

**Component Object Model (COM)** An object-based programming model designed to promote software interoperability; it allows two or more applications or components to easily cooperate with one another, even if they were written by different vendors, at different times, in different programming languages, or if they are running on different computers running different operating systems. OLE technology and ActiveX are both built on top of COM. See also ActiveX.

**concrete class** In Windows Management Instrumentation (WMI), a class from which you can create an instance because it has a full implementation.

**concurrency** The appearance of simultaneous execution of processes or transactions by interleaving the execution of multiple pieces of work.

**connected user** A user who has access to a computer or a resource across the network.

**console tree** The left pane in Microsoft Management Console (MMC) that displays the items contained in the console. The items in the console tree and their hierarchical organization determine the capabilities of a console. See also details pane.

**cookie** A block of data that a Web server stores on a client system. When a user returns to the same Web site, the browser sends a copy of the cookie back to the server. Cookies identify users, instruct the server to send a customized version of the requested Web page, and submit account information for the user.

**credentials** A set of information that includes identification and proof of identification that is used to gain access to local and network resources. Examples of credentials are user names and passwords, smart cards, and certificates. See also certificate.

**CRL** See definition for certificate revocation list (CRL).

**CryptoAPI** An application programming interface (API) that is provided as part of Microsoft Windows. CryptoAPI provides a set of functions that allows applications to encrypt or digitally sign data in a flexible manner while providing protection for the user's sensitive private key data. Actual cryptographic operations are performed by independent modules known as *cryptographic service providers (CSPs)*. See also application programming interface (API); cryptographic service provider (CSP); private key.

**cryptographic service provider (CSP)** The code that performs authentication, encoding, and encryption services that Windows-based applications access through CryptoAPI. A CSP is responsible for creating keys, destroying them, and using them to perform a variety of cryptographic operations. Each CSP provides a different implementation of the CryptoAPI. Some provide stronger cryptographic algorithms, while others use hardware components, such as smart cards. See also authentication; CryptoAPI; encryption.

**cryptography** The processes, art, and science of keeping messages and data secure. Cryptography is used to enable and ensure confidentiality, data integrity, authentication (entity and data origin), and nonrepudiation. See also authentication.

**CSP** See definition for cryptographic service provider (CSP).

**CTL** See definition for certificate trust list (CTL).

**custom property** A metabase property that is not predefined in the metabase schema (MBSchema.xml) and is created programmatically to meet a specific need. See also schema.

**cycle** In logging, to close an existing log file and start a new one.

## D

**daemon** A networking program, usually associated with UNIX systems, that runs in the background performing tool functions such as housekeeping or maintenance without user intervention or awareness. Pronounced "demon."

**Data Encryption Standard (DES)** An encryption algorithm that uses a 56-bit key and maps a 64-bit input block to a 64-bit output block. The key appears to be a 64-bit key, but one bit in each of the eight bytes is used for odd parity, resulting in 56 bits of usable key. See also key.

**data source tier** A logical layer that represents a computer running a Database Management System (DBMS), such as a SQL Server database. See also client tier; middle tier.

**datagram** One packet, or unit, of information that includes relevant delivery information, such as the destination address, that is sent through a packet-switching network. See also packet.

**DCOM** See definition for Distributed Component Object Model (DCOM).

deadlock A situation in which a thread will not relinquish its exclusive access to a critical section.

debugger A program designed to aid in detecting, locating, and correcting errors in another program by allowing the programmer to step through the program, examine the data, and monitor conditions such as the values of variables.

decryption The process of making encrypted data readable again by converting ciphertext to plaintext. See also encryption; plaintext.

default document The file that is sent by a Web server when it receives a request for a Uniform Resource Locator (URL) that does not specify a file name. This document can be generated automatically by the server, or it can be a custom file that is placed in that directory by the administrator. Sometimes called a default home page.

default gateway A configuration item for the TCP/IP protocol that is the IP address of a directly reachable IP router. Configuring a default gateway creates a default route in the IP routing table. See also Internet Protocol (IP); IP address; Transmission Control Protocol/Internet Protocol (TCP/IP).

DES See definition for Data Encryption Standard (DES).

details pane The right pane in Microsoft Management Console (MMC) that displays details for the selected item in the console tree. The details can be a list of items or they can be administrative properties, services, and events that are acted on by a snap-in. See also console tree; snap-in.

DHCP See definition for Dynamic Host Configuration Protocol (DHCP).

dial-up connection The connection to your network if you use a device that uses the telephone network. This includes modems with a standard telephone line, ISDN cards with high-speed ISDN lines, or X.25 networks.

If you are a typical user, you might have one or two dial-up connections, for example, to the Internet and to your corporate network. In a more complex server situation, multiple network modem connections might be used to implement advanced routing.

See also Integrated Services Digital Network (ISDN); modem (modulator/demodulator).

dial-up networking (DUN) Connecting to a remote network or the Internet through a dial-up connection, such as a modem.

Digest authentication An authentication mechanism that hashes user name, password, and other data before transmitting it over the network. See also authentication; Basic authentication; encryption; hash.

digital certificate An electronic certification issued by certification authorities that shows where a program comes from and proves that the installation package has not been altered. Administrators should sign their code with a digital certificate if planning to distribute an Internet Explorer package over the Internet. See also certification authority (CA).

digital signature The part of a digital certificate that contains an encryption key that uniquely identifies the holder of the certificate. See also certificate; client; key pair.

directory An information source that contains information about users, computer files, or other objects. In a file system, a directory stores information about files. In a distributed computing environment (such as a Windows domain), the directory stores information about objects such as printers, fax servers, applications, databases, and other users. See also domain; object.

directory browsing A feature that automatically provides a default Web page of available directories and files to browsers that submit a Uniform Resource Locator (URL) that does not specify a particular file.

directory partition A contiguous subtree of Active Directory that is replicated as a unit to other domain controllers in the forest that contain a replica of the same subtree. In Active Directory, a single domain controller always holds at least three directory partitions: schema (class and attribute definitions for the directory), configuration (replication topology and related metadata), and domain (subtree that contains the per-domain objects for one domain). Domain controllers running Windows Server 2003 can also store one or more application directory partitions. See also Active Directory; attribute; domain.

**directory replication** The copying of a master set of directories from a server (called an export server) to specified servers or workstations (called import computers) in the same or other domains. Replication simplifies the task of maintaining identical sets of directories and files on multiple computers because only a single master copy of the data must be maintained. Files are replicated when they are added to an exported directory and every time a change is saved to the file.

**directory service** Both the directory information source and the service that makes the information available and usable. A directory service enables the user to find an object when given any one of its attributes. See also Active Directory; attribute; directory; object.

**Distributed Component Object Model (DCOM)** The Microsoft Component Object Model (COM) specification that defines how components communicate over Windows-based networks. Use the DCOM Configuration tool to integrate client/server applications across multiple computers. DCOM can also be used to integrate robust Web browser applications. See also Component Object Model (COM).

**distributed processing** A computing environment that contains a client and a server. This structure allows the workload to be divided into parts yet appear as a single process.

**DLL** See definition for dynamic-link library (DLL).

**DNS** See definition for Domain Name System (DNS).

**domain** In Active Directory, a collection of computer, user, and group objects defined by the administrator. These objects share a common directory database, security policies, and security relationships with other domains.

In DNS, any tree or subtree within the DNS namespace. Although the names for DNS domains often correspond to Active Directory domains, DNS domains should not be confused with Active Directory domains.

See also Active Directory; Domain Name System (DNS); object.

**domain controller** In an Active Directory forest, a server that contains a writable copy of the Active Directory database, participates in Active Directory replication, and controls access to network resources. Administrators can manage user accounts, network access, shared resources, site topology, and other directory objects from any domain controller in the forest. See also Active Directory; authentication; directory; forest; shared resource.

**domain name** The name given by an administrator to a collection of networked computers that share a common directory. Part of the DNS naming structure, domain names consist of a sequence of name labels separated by periods. See also domain; Domain Name System (DNS).

**Domain Name System (DNS)** A hierarchical, distributed database that contains mappings of DNS domain names to various types of data, such as IP addresses. DNS enables the location of computers and services by user-friendly names, and it also enables the discovery of other information stored in the database. See also domain name; IP address; ping; Transmission Control Protocol/Internet Protocol (TCP/IP).

**DWORD** A data type that is composed of hexadecimal data with a maximum allotted space of 4 bytes.

**dynamic binding** Binding (converting symbolic addresses in the program to storage-related addresses) that occurs during program execution. The term often refers to object-oriented applications that determine, during run time, which software routines to call for particular data objects. Also called late binding.

**Dynamic Host Configuration Protocol (DHCP)** A TCP/IP service protocol that offers dynamic leased configuration of host IP addresses and distributes other configuration parameters to eligible network clients. DHCP provides safe, reliable, and simple TCP/IP network configuration, prevents address conflicts, and helps conserve the use of client IP addresses on the network.

DHCP uses a client/server model where the DHCP server maintains centralized management of IP addresses that are used on the network. DHCP-supporting clients can then request and obtain lease of an IP address from a DHCP server as part of their network boot process.

See also IP address; Transmission Control Protocol/Internet Protocol (TCP/IP).

**Dynamic HTML** A collection of features that extends the capabilities of traditional HTML, giving Web authors more flexibility, design options, and creative control over the appearance and behavior of Web pages.

dynamic page A Hypertext Markup Language (HTML) document that contains animated GIFs, Java applets, ActiveX Controls, or dynamic HTML (DHTML). Also, a Web page that is created automatically, based on information that is provided by the user, or that is generated "on the fly" with Active Server Pages (ASP).

dynamic-link library (DLL) An operating system feature that allows executable routines (generally serving a specific function or set of functions) to be stored separately as files with .dll extensions. These routines are loaded only when needed by the program that calls them.

## E

early binding Occurs when an object is assigned to a variable that is declared to be of a specific object type. Early bound objects allow the compiler to allocate memory and perform other optimizations before an application executes.

encapsulation The method used to pass data from one protocol over a network within a different protocol. Data from one protocol is wrapped with the header of a different protocol. Encapsulation is described in RFC 1483. See also protocol.

encryption The process of disguising a message or data in such a way as to hide its substance. See also public key encryption; symmetric encryption.

encryption key A bit string that is used in conjunction with an encryption algorithm to encrypt and decrypt data. See also private key; public key.

Ethernet The IEEE 802.3 standard that uses Carrier Sense Multiple Access with Collision Detection (CSMA/CD) as the medium access control. Ethernet supports different mediums, such as coaxial cable, fiber-optic cable, and twisted-pair wiring, and different data rates, such as 10 megabits per second (Mbps).

event Any significant occurrence in the system or an application that requires users to be notified or an entry to be added to a log.

Event Log service A service that records events in the system, security, and application logs. The Event Log service is located in Event Viewer. See also event; event logging; Event Viewer.

event logging The process of recording an audit entry in the audit trail whenever certain events occur, such as services starting and stopping or users logging on and off and accessing resources. See also auditing; event; Event Viewer.

Event Viewer A component you can use to view and manage event logs, gather information about hardware and software problems, and monitor security events. Event Viewer maintains logs about program, security, and system events. See also event; event logging.

extended partition A type of partition that you can create only on basic master boot record (MBR) disks. Extended partitions are useful if you want to create more than four volumes on a basic MBR disk. Unlike primary partitions, you do not format an extended partition with a file system and then assign a drive letter to it. Instead, you create one or more logical drives within the extended partition. After you create a logical drive, you format it and assign it a drive letter. An MBR disk can have up to four primary partitions or three primary partitions, one extended partition, and multiple logical drives. See also logical drive; partition.

Extensible Markup Language (XML) A meta-markup language that provides a format for describing structured data. This facilitates more precise declarations of content and more meaningful search results across multiple platforms. In addition, XML enables a new generation of Web-based data viewing and manipulation applications. See also Hypertext Markup Language (HTML).

extranet A limited subset of computers or users on a public network, typically the Internet, that can access an organization's internal network. For example, the computers or users might belong to a partner organization.

## F

failback The process of moving resources, either individually or in a group, back to their preferred node after the node has failed and come back online. See also node.

failover In server clusters, the process of taking resource groups offline on one node and bringing them online on another node. When failover occurs, all resources within a resource group fail over in a predefined order; resources that depend on other resources are taken offline before, and are brought back online after, the resources on which they depend. See also node; server cluster.

FAT See definition for file allocation table (FAT).

fat server In a client/server architecture, a server that performs most of the processing, with the client performing little or no processing.

**FAT32** A derivative of the file allocation table (FAT) file system. FAT32 supports smaller cluster sizes and larger volumes than FAT, which results in more efficient space allocation on FAT32 volumes. See also file allocation table (FAT).

**fault tolerance** The ability of computer hardware or software to ensure data integrity when hardware failures occur. Fault-tolerant features appear in many server operating systems and include mirrored volumes, RAID-5 volumes, and server clusters. See also cluster.

**file allocation table (FAT)** A file system used by MS-DOS and other Windows operating systems to organize and manage files. The file allocation table is a data structure that Windows creates when you format a volume by using FAT or FAT32 file systems. Windows stores information about each file in the file allocation table so that it can retrieve the file later. See also FAT32; NTFS file system.

**File Transfer Protocol (FTP)** A member of the TCP/IP suite of protocols, used to copy files between two computers on the Internet. Both computers must support their respective FTP roles: one must be an FTP client and the other an FTP server. See also Transmission Control Protocol/Internet Protocol (TCP/IP).

**filter** For Indexing Service, software that extracts content and property values from a document to index them.

For Internet Protocol security (IPSec), a specification of Internet Protocol (IP) traffic that provides the ability to trigger security negotiations for a communication based on the source, destination, and type of IP traffic.

For Internet Information Services (IIS), a feature of Internet Server Application Programming Interface (ISAPI) that allows preprocessing of requests and postprocessing of responses, permitting site-specific handling of Hypertext Transfer Protocol (HTTP) requests and responses.

In IP and Internetwork Packet Exchange (IPX) packet filtering, a definition in a series of definitions that indicates to the router the type of traffic allowed or disallowed on each interface.

See also Internet Information Services (IIS); Internet Protocol (IP); Internet Protocol security (IPSec); Internet Server Application Programming Interface (ISAPI).

**firewall** A combination of hardware and software that provides a security system for the flow of network traffic, usually to prevent unauthorized access from outside to an internal network or intranet. Also called a *security-edge gateway*. See also proxy server.

**forest** One or more Active Directory domains that share the same class and attribute definitions (schema), site and replication information (configuration), and forest-wide search capabilities (global catalog). Domains in the same forest are linked with two-way, transitive trust relationships. See also Active Directory; domain.

**FORTEZZA** A family of security products including PCMCIA-based cards, compatible serial port devices, combination cards (such as FORTEZZA/Modem and FORTEZZA/Ethernet), server boards, and others. FORTEZZA is a registered trademark held by the U.S. National Security Agency.

**frame** In synchronous communication, a package of information transmitted as a single unit from one device to another.

**FTP** See definition for File Transfer Protocol (FTP).

## G

**gateway** A dedicated device (or a set of services running on a dedicated computer) that routes network traffic and enables communication between different networking protocols. A gateway is a multiprotocol Internet Protocol (IP) router that translates between different transport protocols or data formats. See also Internet Protocol (IP).

**globally unique identifier (GUID)** A 16-byte value generated from the unique identifier on a device, the current date and time, and a sequence number. A GUID is used to identify a particular device or component.

**graphical user interface (GUI)** A display format, like that of Windows, that represents a program’s functions with graphic images such as buttons and icons. GUIs enable a user to perform operations and make choices by pointing and clicking with a mouse.

group A collection of users, computers, contacts, and other groups. Groups can be used as security or as e-mail distribution collections. Distribution groups are used only for e-mail. Security groups are used both to grant access to resources and as e-mail distribution lists. See also domain; local group.

group account A collection of user accounts. By making a user account a member of a group, you give the related user all the rights and permissions granted to the group. See also group.

Group Policy The infrastructure within Active Directory directory service that enables directory-based change and configuration management of user and computer settings, including security and user data. You use Group Policy to define configurations for groups of users and computers. With Group Policy, you can specify policy settings for registry-based policies, security, software installation, scripts, folder redirection, remote installation services, and Internet Explorer maintenance. The Group Policy settings that you create are contained in a Group Policy object (GPO). By associating a GPO with selected Active Directory system containers—sites, domains, and organizational units—you can apply the GPO's policy settings to the users and computers in those Active Directory containers. To create an individual GPO, use the Group Policy Object Editor. To manage Group Policy objects across an enterprise, you can use the Group Policy Management console. See also Active Directory.

Guest account A built-in account used to log on to a computer running Windows when a user does not have an account on the computer or domain or in any of the domains trusted by the computer's domain. See also domain.

GUID See definition for globally unique identifier (GUID).

## H

hash A fixed-size result that is obtained by applying a one-way mathematical function (sometimes called a *hash algorithm*) to an arbitrary amount of data. If there is a change in the input data, the hash changes. The hash can be used in many operations, including authentication and digital signing. Also called a *message digest*. See also authentication; hash algorithm.

hash algorithm An algorithm that produces a hash value of some piece of data, such as a message or session key. With a good hash algorithm, changes in the input data can change every bit in the resulting hash value; for this reason, hashes are useful in detecting any modification in a data object, such as a message. Furthermore, a good hash algorithm makes it computationally infeasible to construct two independent inputs that have the same hash. Typical hash algorithms include MD2, MD4, MD5, and SHA-1. Also called a *hash function*. See also MD5; Secure Hash Algorithm (SHA-1).

headless server See definition for remotely administered server.

heaps A portion of memory reserved for a program to use for the temporary storage of data structures whose existence or size cannot be determined until the program is running.

Help and Support Center A unified place where a user can access all Help and Support content and services from both Microsoft and the OEM.

hexadecimal A base-16 number system represented by the digits 0 through 9 and the uppercase or lowercase letters A (equivalent to decimal 10) through F (equivalent to decimal 15).

home directory The root directory for a Web site, where the content files are stored. Also called a document root or Web root. In Internet Information Services (IIS), the home directory and all its subdirectories are available to users by default. Also, the root directory for an IIS service. Typically, the home directory for a site contains the home page. See also home page.

home page In the context of Internet Explorer, the home page is the first page users see when they start the browser. "Home page" is also a more general term for the main page of a Web site, which usually contains a main menu or table of contents with links to other pages within the site.

host Any device on a TCP/IP network that has an Internet Protocol (IP) address. Examples of hosts include servers, workstations, network-interface print devices, and routers. Sometimes used to refer to a specific network computer that is running a service used by network or remote clients.

For Network Load Balancing, a cluster consists of multiple hosts connected over a local area network (LAN).

See also client; cluster; local area network (LAN); Network Load Balancing; server; Transmission Control Protocol/Internet Protocol (TCP/IP).

host name The DNS name of a device on a network. These names are used to locate computers on the network. To find another computer, its host name must either appear in the Hosts file or be known by a DNS server. For most Windows-based computers, the host name and the computer name are the same. See also Domain Name System (DNS).

hotfix An update to address an issue identified after a software product has been distributed. Hotfix distribution is limited by its licensing terms.

HTML See definition for Hypertext Markup Language (HTML).

HTTP See definition for Hypertext Transfer Protocol (HTTP).

HTTP header An informational listing at the top of a Hypertext Transfer Protocol (HTTP) request or response.

HTTPS See definition for Secure Hypertext Transfer Protocol.

Hypertext Markup Language (HTML) A simple markup language used to create hypertext documents that are portable from one platform to another. HTML files are simple ASCII text files with codes embedded (indicated by markup tags) to denote formatting and hypertext links. See also American Standard Code for Information Interchange (ASCII).

Hypertext Transfer Protocol (HTTP) The protocol used to transfer information on the World Wide Web. An HTTP address (one kind of Uniform Resource Locator (URL)) takes the following form: http://www.microsoft.com. See also protocol.

## I

ICMP See definition for Internet Control Message Protocol (ICMP).

identities, multiple See definition for multiple identities.

identity A person or entity that must be verified by means of authentication, based on criteria such as a password or a certificate. See also authentication; certificate.

IEEE Institute of Electrical and Electronics Engineers, founded in 1963. IEEE is an organization composed of engineers, scientists, and students, best known for developing standards for the computer and electronics industry.

IETF See definition for Internet Engineering Task Force (IETF).

IIS See definition for Internet Information Services (IIS).

IIS 5.0 isolation mode Internet Information Services (IIS) 6.0 isolation mode that simulates the IIS 5.0 Web process model.

IIS Admin Objects A set of methods, provided by Internet Information Services (IIS), that allow applications to access and modify configuration settings in the metabase.

IIS Server Instance resource A server-instance designation used with Internet Information Services (IIS) that supports the WWW and FTP services. IIS server instances are supported as cluster resources by a Resource DLL. IIS Server Instance resources can have dependencies on IP Address resources, Network Name resources, and Physical Disk resources. Access information for server instances does not fail over. See also failover; Internet Information Services (IIS).

impersonation A circumstance that occurs when Windows allows one process to take on the security attributes of another. See also attribute; security.

impersonation token An access token that captures the security information of a client process, allowing a service to "impersonate" the client process in security operations.

in-memory metabase An image of the Internet Information Services (IIS) metabase that has been loaded from disk into the computer's RAM memory and is used while IIS is running. See also metabase.

in-process Internet Server API (ISAPI) extensions that are hosted in the worker process address space. See also Internet Server Application Programming Interface (ISAPI).

in-schema property A metabase property predefined in the metabase schema (MBSchema.xml) file. See also metabase schema.

inheritance In security, a mechanism that allows a specific access control entry (ACE) to be copied from the container where it was applied to all children of the container. Inheritance can be used to manage access to a whole subtree of objects in a single update operation.

In Active Directory, the ability to build new object classes from existing object classes. The new object is defined as a subclass of the original object class. The original object class becomes a superclass of the new object. A subclass inherits the attributes of the superclass, including structure rules and content rules.

In Group Policy, a mechanism that allows policy settings in Group Policy objects (GPOs) that are linked to parent containers to be applied to objects in child containers.

See also Active Directory.

**input/output (I/O) port** A channel through which data is transferred between a device and the microprocessor. The port appears to the microprocessor as one or more memory addresses that it can use to send or receive data.

**Integrated Services Digital Network (ISDN)** A digital phone line used to provide higher bandwidth. ISDN in North America is typically available in two forms: Basic Rate Interface (BRI) consists of 2 B-channels at 64 kilobits per second (Kbps) and a D-channel at 16 Kbps; Primary Rate Interface (PRI) consists of 23 B-channels at 64 Kbps and a D-channel at 64 Kbps. An ISDN line must be installed by the phone company at both the calling site and the called site.

**Integrated Windows authentication** A configuration setting that enables negotiation of authentication protocols in Internet Information Services (IIS). See also Internet Information Services (IIS).

**internet** *internet*. Two or more network segments connected by routers. Another term for *internetwork*.

*Internet*. A worldwide network of computers. If you have access to the Internet, you can retrieve information from millions of sources, including schools, governments, businesses, and individuals.

**Internet Control Message Protocol (ICMP)** A required maintenance protocol in the TCP/IP suite that reports errors and provides simple diagnostic capabilities. ICMP is used by the Ping tool to perform TCP/IP troubleshooting. See also Internet Protocol (IP); protocol; Transmission Control Protocol/Internet Protocol (TCP/IP).

**Internet Engineering Task Force (IETF)** An open community of network designers, operators, vendors, and researchers concerned with the evolution of Internet architecture and the smooth operation of the Internet. Technical work is performed by working groups organized by topic areas (such as routing, transport, and security) and through mailing lists. Internet standards are developed in IETF Requests for Comments (RFCs), which are a series of notes that discuss many aspects of computing and computer communication, focusing on networking protocols, programs, and concepts.

**Internet Information Services (IIS)** Software services that support Web site creation, configuration, and management, along with other Internet functions. Internet Information Services include Network News Transfer Protocol (NNTP), File Transfer Protocol (FTP), and Simple Mail Transfer Protocol (SMTP). See also File Transfer Protocol (FTP).

**Internet Protocol (IP)** A routable protocol in the TCP/IP protocol suite that is responsible for IP addressing, routing, and the fragmentation and reassembly of IP packets. See also packet; Transmission Control Protocol/Internet Protocol (TCP/IP).

**Internet Protocol security (IPSec)** A set of industry-standard, cryptography-based protection services and protocols. IPSec protects all protocols in the TCP/IP protocol suite except Address Resolution Protocol (ARP). For virtual private network (VPN) connections, IPSec is used in conjunction with Layer Two Tunneling Protocol (L2TP). See also Address Resolution Protocol (ARP); protocol; Transmission Control Protocol/Internet Protocol (TCP/IP).

**Internet Server Application Programming Interface (ISAPI)** An application programming interface (API) that resides on a server computer for initiating software services tuned for Windows operating systems.

In Microsoft Provisioning System, ISAPI resides on the Web server.

See also application programming interface (API).

**Internet service** One of any of a number of technologies for making information accessible to users over the Internet. Each Internet service is defined by a protocol, such as Hypertext Transfer Protocol (HTTP), and each is enabled using client/server applications, such as Web browsers and Web servers. Internet protocols are defined in the Request for Comments (RFC) documents that are published by the Internet Engineering Task Force (IETF).

**Internet service provider (ISP)** A company that provides individuals or companies access to the Internet and the World Wide Web. An ISP provides a telephone number, a user name, a password, and other connection information so users can connect their computers to the ISP's computers. An ISP typically charges a monthly or hourly connection fee.

**intranet** A network within an organization that uses Internet technologies and protocols, but is available only to certain people, such as employees of a company. Also called a *private network*. See also internet.

**IP** See definition for Internet Protocol (IP).

IP address For Internet Protocol version 4 (IPv4), a 32-bit address used to identify an interface on a node on an IPv4 internetwork. Each interface on the IP internetwork must be assigned a unique IPv4 address, which is made up of the network ID, plus a unique host ID. This address is typically represented with the decimal value of each octet separated by a period (for example, 192.168.7.27). You can configure the IP address statically or dynamically by using Dynamic Host Configuration Protocol (DHCP).

For Internet Protocol version 6 (IPv6), an identifier that is assigned at the IPv6 layer to an interface or set of interfaces and that can be used as the source or destination of IPv6 packets.

See also Dynamic Host Configuration Protocol (DHCP); Internet Protocol (IP); node; octet.

IPSec See definition for Internet Protocol security (IPSec).

ISAPI See definition for Internet Server Application Programming Interface (ISAPI).

ISDN See definition for Integrated Services Digital Network (ISDN).

ISP See definition for Internet service provider (ISP).

## J

JIT See definition for just-in-time (JIT) activation.

just-in-time (JIT) activation The ability of a Component Object Model (COM) object to be activated only as needed for executing requests from its client. Objects can be deactivated even while clients hold references to them, allowing otherwise idle server resources to be used more productively.

## K

Keep-Alive connection A Hypertext Transfer Protocol (HTTP) connection that is not closed after an exchange is completed.

Kerberos V5 authentication protocol An authentication mechanism used to verify user or host identity. The Kerberos V5 authentication protocol is the default authentication service. Internet Protocol security (IPSec) can use the Kerberos protocol for authentication. See also Internet Protocol security (IPSec).

kernel The core of layered architecture that manages the most basic operations of the operating system and the computer's processor. The kernel schedules different blocks of executing code, called threads, for the processor to keep it as busy as possible and coordinates multiple processors to optimize performance. The kernel also synchronizes activities among Executive-level subcomponents, such as I/O Manager and Process Manager, and handles hardware exceptions and other hardware-dependent functions. The kernel works closely with the hardware abstraction layer.

kernel mode A highly privileged mode of operation where program code has direct access to all memory, including the address spaces of all user-mode processes and applications, and to hardware. Also known as *supervisor mode*, *protected mode*, or *Ring 0*.

key In Registry Editor, a folder that appears in the left pane of the Registry Editor window. A key can contain subkeys and entries. For example, Environment is a key of **HKEY_CURRENT_USER**.

In IP security (IPSec), a value used in combination with an algorithm to encrypt or decrypt data. Key settings for IPSec are configurable to provide greater security.

See also Internet Protocol security (IPSec); registry; subkey.

key pair A private key and its related public key. See also private key; public key.

## L

late binding See definition for dynamic binding.

LCID See definition for Locale Identifier (LCID).

LDAP See definition for Lightweight Directory Access Protocol (LDAP).

Lightweight Directory Access Protocol (LDAP) The primary access protocol for Active Directory. LDAP is an industry-standard protocol, established by the Internet Engineering Task Force (IETF), that allows users to query and update information in a directory service. Active Directory supports both LDAP version 2 and LDAP version 3. See also Active Directory; directory service; Internet Engineering Task Force (IETF); protocol.

load balancing A technique used by Windows Clustering to scale the performance of a server-based program (such as a Web server) by distributing its client requests across multiple servers within the cluster. Each host can specify the load percentage that it will handle, or the load can be equally distributed across all the hosts. If a host fails, Windows Clustering dynamically redistributes the load among the remaining hosts. See also cluster; host.

local area network (LAN) A communications network connecting a group of computers, printers, and other devices located within a relatively limited area (for example, a building). A LAN enables any connected device to interact with any other on the network.

local group A security group that can be granted rights and permissions on only resources on the computer on which the group is created. Local groups can have any user accounts that are local to the computer as members, as well as users, groups, and computers from a domain to which the computer belongs.

Locale Identifier (LCID) A unique integer that represents a locale for the formatting style of dates, times, currencies and other values, which is different for each geographical location. In Internet Information Services (IIS), the default LCID is the same as the system locale. See also LOCALE_SYSTEM_DEFAULT.

LOCALE_SYSTEM_DEFAULT The default system locale. There is also a default user locale. See also Locale Identifier (LCID).

LocalHost A placeholder for the name of the computer on which a program is running. LocalHost uses the reserved loopback IP address (127.0.0.1 in IPv4 and ::1 in IPv6).

log file A file that stores messages generated by an application, service, or operating system. These messages are used to track the operations performed. For example, Web servers maintain log files listing every request made to the server. Log files are usually plain text (ASCII) files and often have a .log extension.

In Backup, a file that contains a record of the date the tapes were created and the names of files and directories successfully backed up and restored. The Performance Logs and Alerts service also creates log files.

See also American Standard Code for Information Interchange (ASCII).

logical drive A volume that you create within an extended partition on a basic master boot record (MBR) disk. Logical drives are similar to primary partitions, except that you are limited to four primary partitions per disk, whereas you can create an unlimited number of logical drives per disk. A logical drive can be formatted and assigned a drive letter. See also extended partition.

## M

Mail or Messaging Application Programming Interface (MAPI) An open and comprehensive messaging interface that is used by developers to create messaging and workgroup applications, such as e-mail, scheduling, calendars, and document management. In a distributed client/server environment, MAPI provides enterprise messaging services within Windows Open Services Architecture (WOSA).

malicious user A person who has legitimate access to a system and poses a security threat to it, such as someone who tries to elevate their user rights to gain access to unauthorized data. See also security; user rights.

Management Information Base (MIB) Information about aspects of a network that can be managed by using the Simple Network Management Protocol (SNMP). This information is formatted in MIB files that are provided for each service that can be monitored. Most third-party monitors (clients) use SNMP and MIB files to monitor Web, File Transfer Protocol (FTP), and other Windows services. Using SNMP, developers or system administrators can write their own custom monitoring applications.

MAPI See definition for Mail or Messaging Application Programming Interface (MAPI).

master properties In Internet Information Services (IIS), properties that are set at the computer level that become default settings for all Web or File Transfer Protocol (FTP) sites on that computer. See also inheritance.

MD5 An industry-standard one-way, 128-bit hashing scheme, developed by RSA Data Security, Inc., and used by various Point-to-Point Protocol (PPP) vendors for encrypted authentication. A hashing scheme is a method for transforming data (for example, a password) in such a way that the result is unique and cannot be changed back to its original form. The Challenge Handshake Authentication Protocol (CHAP) uses challenge-response with one-way MD5 hashing on the response. In this way, you can prove to the server that you know your password without actually sending the password over the network. See also hash algorithm; MD5.

MDAC See definition for Microsoft Data Access Components (MDAC).

**Message Queuing** A message queuing and routing system for Windows that enables distributed applications running at different times to communicate across heterogeneous networks and with computers that may be offline. Message Queuing provides guaranteed message delivery, efficient routing, security, and priority-based messaging. Formerly known as *MSMQ*.

**metabase** A hierarchical store of configuration information and schema that is used to configure Internet Information Services (IIS). The metabase performs some of the same functions as the system registry, but it uses less disk space. In physical terms, the metabase is a combination of the MetaBase.xml and MBSchema.xml files and the in-memory metabase.

**metabase configuration file** A file that stores Internet Information Services (IIS) configuration settings to disk. This file is named MetaBase.xml by default. When IIS is started or restarted, the configuration settings are read from MetaBase.xml into the IIS cache in memory, which is called the in-memory metabase.

**metabase schema** The master configuration file (MBSchema.xml) supplied with Internet Information Services (IIS) that contains all of the predefined properties from which metabase entries are derived.

**metadata** Data that is used to describe other data. For example, Indexing Service must maintain data that describes the data in the content index.

**method** A procedure (function) that acts on an object.

**MIB** See definition for Management Information Base (MIB).

**Microsoft Data Access Components (MDAC)** Consists of ActiveX Data Objects (ADO), the Remote Data Service (RDS), Microsoft OLE DB Provider for ODBC, Open Database Connectivity (ODBC), ODBC drivers for Microsoft SQL Server, Microsoft Access and other desktop databases, as well as Oracle databases.

**middle tier** The logical layer between a user interface or Web client and the database. This is typically where the Web server resides and where business objects are instantiated. Also known as *application server tier*. See also client tier; data source tier.

**modem (modulator/ demodulator)** A device that enables computer information to be transmitted and received over a telephone line. The transmitting modem translates digital computer data into analog signals that can be carried over a telephone line. The receiving modem translates the analog signals back to digital form.

**MSMQ** See definition for Message Queuing.

**MTA** See definition for multithreaded apartment (MTA).

**multiple identities** Multiple Web sites that are hosted on one computer. Also called virtual servers.

**Multipurpose Internet Mail Extensions mapping (MIME mapping)** A method of configuring browsers to view files that are in multiple formats. An extension of the Internet mail protocol that enables the sending of 8-bit-based e-mail messages, which are used to support extended character sets, voice mail, facsimile images, and so on.

**multithreaded apartment (MTA)** A form of multithreading that is supported by Component Object Model (COM). In a multithreaded apartment model, all of the threads in the process that have been initialized as free-threaded reside in a single apartment.

**multithreading** Running several processes in rapid sequence within a single program, regardless of which logical method of multitasking is being used by the operating system. Because the user's sense of time is much slower than the processing speed of a computer, multitasking appears to be simultaneous, even though only one task at a time can use a computer processing cycle.

## N

**name resolution** The process of having software translate between names that are easy for users to work with and numerical IP addresses, which are difficult for users but necessary for TCP/IP communications. Name resolution can be provided by software components such as DNS or WINS. See also Domain Name System (DNS); Transmission Control Protocol/Internet Protocol (TCP/IP); Windows Internet Name Service (WINS).

**namespace** A naming convention that defines a set of unique names for resources in a network. For DNS, a hierarchical naming structure that identifies each network resource and its place in the hierarchy of the namespace. For WINS, a flat naming structure that identifies each network resource using a single, unique name. See also Domain Name System (DNS); Windows Internet Name Service (WINS).

Network File System (NFS) A service for distributed computing systems that provides a distributed file system, eliminating the need for keeping multiple copies of files on separate computers.

network latency The time it takes for information to be transferred between computers in a network.

Network Load Balancing A Windows network component that uses a distributed algorithm to load-balance Internet Protocol (IP) traffic across a number of hosts, helping to enhance the scalability and availability of mission-critical, IP-based services, such as Terminal Services, Web services, virtual private networking, and streaming media. It also provides high availability by detecting host failures and automatically redistributing traffic to the surviving hosts. See also availability; cluster; host; scalability.

Network News Transfer Protocol (NNTP) A protocol that is used to distribute network news messages to NNTP servers and to NNTP clients (news readers) on the Internet. NNTP provides for the distribution, inquiry, retrieval, and posting of news articles by using a reliable, stream-based transmission of news on the Internet. NNTP is designed in such a way that news articles are stored on a server in a central database, so that users can select specific items to read. Indexing, cross-referencing, and expiration of old messages are also provided. NNTP is defined in RFC 977.

NNTP See definition for Network News Transfer Protocol (NNTP).

node For tree structures, a location on the tree that can have links to one or more items below it.

For local area networks (LANs), a device that is connected to the network and is capable of communicating with other network devices.

For server clusters, a computer system that is an active or inactive member of a cluster.

See also local area network (LAN); server cluster.

NTFS file system An advanced file system that provides performance, security, reliability, and advanced features that are not found in any version of file allocation table (FAT). For example, NTFS guarantees volume consistency by using standard transaction logging and recovery techniques. If a system fails, NTFS uses its log file and checkpoint information to restore the consistency of the file system. NTFS also provides advanced features, such as file and folder permissions, encryption, disk quotas, and compression. See also FAT32; file allocation table (FAT).

## O

object An entity, such as a file, folder, shared folder, printer, or Active Directory object, described by a distinct, named set of attributes. For example, the attributes of a File object include its name, location, and size; the attributes of an Active Directory User object might include the user's first name, last name, and e-mail address.

For OLE and ActiveX, an object can also be any piece of information that can be linked to, or embedded into, another object.

See also Active Directory; attribute.

object identifier (OID) An extensible, unique identification number for attributes and classes. Performance counter names have their own object identifiers, which are listed in Management Information Base (MIB) files, to provide performance monitoring applications with access to the counters. See also Management Information Base (MIB); Simple Network Management Protocol (SNMP).

Object Linking and Embedding (OLE) A set of integration standards for transferring and sharing information among client applications. Also, a protocol that enables the creation of compound documents with embedded links to applications, so that a user does not have to switch among applications to make revisions. OLE is based on the Component Object Model (COM), and it enables the development of reusable objects that operate across multiple applications.

Object Linking and Embedding Database (OLE DB) Data-access interfaces that provide consistent access to Structured Query Language (SQL) data sources and non-SQL data sources across an organization and the Internet. See also structured query language (SQL).

object-cache scavenger The code that periodically scans the cache for objects to be discarded. It deletes files that have not been used recently and therefore are unlikely to be used again in the near future.

octet In programming, an octet refers to eight bits or one byte. IP addresses, for example, are typically represented in dotted-decimal notation; that is, with the decimal value of each octet of the address separated by a period.

ODBC See definition for Open Database Connectivity (ODBC).

OID See definition for object identifier (OID).

OLE See definition for Object Linking and Embedding (OLE).

OLE DB See definition for Object Linking and Embedding Database (OLE DB).

Open Database Connectivity (ODBC) An application programming interface (API) that enables applications to access data from a variety of existing data sources. A standard specification for cross-platform database access.

out-of-process For IIS 5.0 isolation mode, ISAPI extensions that are hosted in a surrogate process called DLLHOST.exe, which is managed by COM+. See also IIS 5.0 isolation mode.

out-of-process component A Component Object Model (COM) component that runs in a separate process space from its client. See also process isolation.

out-of-process, pooled See definition for pooled out-of-process.

## P-Q

packet An Open Systems Interconnection (OSI) network layer transmission unit that consists of binary information representing both data and a header containing an identification number, source and destination addresses, and error-control data.

page See definition for Web page.

parameter A value that is passed in a function call.

partition A portion of a physical disk that functions as though it were a physically separate disk. After you create a partition, you must format it and assign it a drive letter before you can store data on it.

On basic disks, partitions are known as basic volumes, which include primary partitions and logical drives. On dynamic disks, partitions are known as dynamic volumes, which include simple, striped, spanned, mirrored, and RAID-5 volumes.

See also extended partition.

password authentication See definition for authentication.

path, physical See definition for physical path.

path, relative See definition for relative path.

performance counter In System Monitor, a data item that is associated with a performance object. For each counter selected, System Monitor presents a value corresponding to a particular aspect of the performance that is defined for the performance object.

Perl (Practical Extraction and Report Language) An interpreted language that is based on C and several UNIX utilities. Perl has powerful string-handling features for extracting information from text files. Perl can assemble a string and send it to the shell as a command; therefore, it is often used for system administration tasks. A program in Perl is known as a script. Perl was devised by Larry Wall at the NASA Jet Propulsion Laboratory. See also script.

permission A rule associated with an object to regulate which users can gain access to the object and in what manner. Permissions are assigned or denied by the object's owner. See also object.

physical path A universal naming convention (UNC) directory path. See also relative path.

ping A utility that verifies connections to one or more remote hosts. The ping command uses Internet Control Message Protocol (ICMP) echo request and echo reply packets to determine whether a particular Internet Protocol (IP) system on a network is functional. **Ping** is useful for diagnosing IP network or router failures. See also host; Internet Control Message Protocol (ICMP); Internet Protocol (IP); packet.

plaintext Data that is not encrypted. Sometimes also called *cleartext*. See also encryption.

Point-to-Point Protocol (PPP) A set of industry-standard framing and authentication protocols that are included with Windows to ensure interoperability with other remote access software. PPP negotiates configuration parameters for multiple layers of the Open Systems Interconnection (OSI) model. The Internet standard for serial communications, PPP defines how data packets are exchanged with other Internet-based systems using a modem connection.

Point-to-Point Tunneling Protocol (PPTP) A specification for virtual private networks (VPNs) in which some nodes of a local area network (LAN) are connected through the Internet. PPTP is an open industry standard that supports widely used networking protocols: Internet Protocol (IP), Internetwork Packet Exchange (IPX), and Microsoft NetBIOS Extended User Interface (NetBEUI). Organizations can use PPTP to outsource their remote dial-up needs to an Internet service provider or to other carriers to reduce cost and complexity.

**policies** Conditions that are set by the system administrator, for example, how quickly account passwords expire and how many unsuccessful logon attempts are allowed before a user is locked out. Policies manage accounts to help prevent exhaustive or random password attacks.

**pooled out-of-process** For IIS 5.0 isolation mode, a special Web Application Manager (WAM) package that hosts all out-of-process ISAPI extensions that are set to medium isolation within the same DLLHOST.exe process. See also IIS 5.0 isolation mode; out-of-process; Web Application Manager (WAM).

**port number** A number that identifies a certain Internet application. For example, the default port number for the WWW service is 80.

**PPP** See definition for Point-to-Point Protocol (PPP).

**PPTP** See definition for Point-to-Point Tunneling Protocol (PPTP).

**private key** The secret half of a cryptographic key pair that is used with a public key algorithm. Private keys are typically used to decrypt a symmetric session key, digitally sign data, or decrypt data that has been encrypted with the corresponding public key. See also public key; public key encryption.

**process** An operating system object that consists of an executable program, a set of virtual memory addresses, and one or more threads. When a program runs, a process is created.

**process accounting** A feature of Internet Information Services (IIS) that administrators can use to monitor and log resource consumption of Common Gateway Interface (CGI) scripts and out-of-process applications.

**process isolation** Running an application or component out of process. See also out-of-process component.

**property inheritance** See definition for inheritance.

**protocol** A set of rules and conventions for sending information over a network. These rules govern the content, format, timing, sequencing, and error control of messages exchanged among network devices. See also Internet Protocol (IP); Transmission Control Protocol/Internet Protocol (TCP/IP).

**provider** See definition for WMI provider.

**proxy** A software program that connects a user to a remote destination through an intermediary gateway.

**proxy server** A firewall component that manages Internet traffic to and from a local area network (LAN) and that can provide other features, such as document caching and access control. A proxy server can improve performance by supplying frequently requested data, such as a popular Web page, and it can filter and discard requests that the owner does not consider appropriate, such as requests for unauthorized access to proprietary files. See also firewall; local area network (LAN).

**public key** The nonsecret half of a cryptographic key pair that is used with a public key algorithm. Public keys are typically used when encrypting a session key, verifying a digital signature, or encrypting data that can be decrypted with the corresponding private key. See also key; private key; public key encryption.

**public key encryption** A method of encryption that uses two encryption keys that are mathematically related. One key is called the *private key* and is kept confidential. The other is called the *public key* and is freely given out to all potential correspondents. In a typical scenario, a sender uses the receiver's public key to encrypt a message. Only the receiver has the related private key to decrypt the message. The complexity of the relationship between the public key and the private key means that, provided the keys are long enough, it is computationally infeasible to determine one from the other. Also called *asymmetric encryption*. See also encryption; private key; public key; symmetric encryption.

**public-key algorithm** An asymmetric cipher that uses two keys, one for encryption, the public key, and the other for decryption, the private key. See also asymmetric key algorithm; decryption; encryption; private key; public key.

## R

**RAID** See definition for Redundant Array of Independent Disks (RAID).

**random access memory (RAM)** Memory that can be read from or written to by a computer or other devices. Information stored in RAM is lost when the computer is turned off.

**realm** A term that is sometimes used for domain, in this case to refer to user domains that are established for security reasons, not Internet domains. For password-protected files, the name of the protected resource or area on the server. If the user tries to access the protected resource while browsing, the name of the realm usually appears in the dialog box that asks for a user name and password.

**redirection** Redirection can be used to automatically send a user from an outdated Uniform Resource Locator (URL) to a new URL.

**Redundant Array of Independent Disks (RAID)** A data storage method in which data, along with information used for error correction, such as parity bits, is distributed among two or more hard disk drives to improve performance and reliability. The hard disk array is governed by array management software and a disk controller, which handles the error correction. RAID is generally used on network servers. Several defined levels of RAID offer differing trade-offs among access speed, reliability, and cost. Windows includes three of the RAID levels: Level 0, Level 1, and Level 5.

**registry** A database repository for information about a computer's configuration. The registry contains information that Windows continually references during operation, such as:

Profiles for each user

The programs installed on the computer and the types of documents that each can create

Property settings for folders and program icons

What hardware exists on the system

Which ports are being used

The registry is organized hierarchically as a tree, and it is made up of keys and their subkeys, hives, and entries.

See also key; subkey.

**relative path** A universal naming convention (UNC) directory path with placeholders, or wildcards, at some levels. Also, the physical path that corresponds to a Uniform Resource Locator (URL). See also physical path.

**remote procedure call (RPC)** In programming, a call by one program to a second program on a remote system. The second program usually performs a task and returns the results of that task to the first program.

**remotely administered server** A server that you can administer by using a different computer. You typically access this type of server by using a network connection. A remotely administered server can have a local keyboard, mouse, or video card and monitor. If it does not have these peripherals attached, it is also known as a *headless server*. Such servers are often housed in a physically secure location. See also server.

**replication** The copying from one server node to another of either content or the configuration metabase, or both. This copying can be done either manually or automatically by using replication software. Replication is a necessary function of clustering that ensures fault tolerance. See also fault tolerance.

**Request for Comments (RFC)** The document series, begun in 1969, that describes the Internet suite of protocols and related experiments. Not all (in fact, very few) RFCs describe Internet standards, but all Internet standards are written up as RFCs. The RFC series of documents is unusual in that the proposed protocols are forwarded by the Internet research and development community, acting on its own behalf, as opposed to the formally reviewed and standardized protocols that are promoted by organizations such as the American National Standards Institute (ANSI).

**router** An intermediary device on a communications network that expedites message delivery. On a single network linking many computers through a mesh of possible connections, a router receives transmitted messages and forwards them to their correct destinations over the most efficient available route. On an interconnected set of local area networks (LANs) using the same communications protocols, a router serves the somewhat different function of acting as a link between LANs, enabling messages to be sent from one LAN to another.

**RPC** See definition for remote procedure call (RPC).

**RSA** A public-key encryption standard for Internet security. This acronym derives from the last names of the inventors of the technology: Rivest, Shamir, and Adleman.

## S

scalability A measure of how well a computer, service, or application can grow to meet increasing performance demands. For server clusters, the ability to incrementally add one or more systems to an existing cluster when the overall load of the cluster exceeds its capabilities. See also server cluster.

schema A representation of the structure of something. Classes in Visual Basic and C++ can be said to be schemas of objects, and objects are instances of classes. In Internet Information Services (IIS), the metabase schema represents the structure of the metabase configuration file.

scope In programming, the extent to which an identifier, such as a constant, data type, variable, or routine, can be referenced within a program. Scope can be global or local. Scope can also be affected by the redefinition of identifiers, for example, by giving the same name to both a global variable and a local variable.

script A kind of program that consists of a set of instructions for an application or utility program. A script can be embedded in a Web page. See also ActiveX; common gateway interface (CGI).

scripting engine A program that interprets and executes a script. See also script.

search expression See Other Definition

search interface See Other Definition

search string See Other Definition

Secure Hash Algorithm (SHA-1) An algorithm that generates a 160-bit hash value from an arbitrary amount of input data. SHA-1 is used with the Digital Signature Algorithm (DSA) in the Digital Signature Standard (DSS), among other places. See also hash algorithm.

Secure Hypertext Transfer Protocol A protocol that provides a secure Hypertext Transfer Protocol (HTTP) connection. See also Hypertext Transfer Protocol (HTTP); protocol.

Secure Sockets Layer (SSL) A protocol that supplies secure data communication through data encryption and decryption. SSL uses RSA public-key encryption for specific TCP/IP ports. It is intended for handling commerce payments. An alternative method is Secure-HTTP (S-HTTP), which is used to encrypt specific Web documents, rather than the entire session. SSL is a general-purpose encryption standard. SSL can also be used for Web applications that require a secure link, such as e-commerce applications, or for controlling access to Web-based subscription services.

security On a network, protection of a computer system and its data from harm or loss, implemented especially so that only authorized users can gain access to shared files. See also authorization.

security context The security attributes or rules that are currently in effect. For example, the rules that govern what a user can do to a protected object are determined by security information in the user's access token and in the object's security descriptor. Together, the access token and the security descriptor form a security context for the user's actions on the object. See also object.

Selectable Cryptographic Service Provider See definition for cryptographic service provider (CSP).

server In general, a computer that provides shared resources to network users. See also client; shared resource.

server certificate A unique digital identification that forms the basis of a Web server's Secure Sockets Layer (SSL) security features. Server certificates are obtained from a mutually trusted, third-party organization, and they provide a way for users to authenticate the identity of a Web site.

server cluster A group of computers, known as *nodes*, working together as a single system to ensure that mission-critical applications and resources remain available to clients. A server cluster presents the appearance of a single server to a client. See also cluster; node.

server node An individual computer in a server cluster.

server process A process that hosts Component Object Model (COM) components. A COM component can be loaded into a surrogate server process, either on the client computer (local) or on another computer (remote). It can also be loaded into a client application process (in-process).

server-side include (SSI) A mechanism for including dynamic text in World Wide Web documents. Server-side includes are special command codes that are recognized and interpreted by the server; their output is placed in the document body before the document is sent to the browser. Server-side includes can be used, for example, to include the Date and Time stamp in the text of the file.

session key A digital key that is created by a client, encrypted, and then sent to a server. This key is used to encrypt data that is sent by the client.

**shared resource** Any device, data, or program that is used by more than one program or one other device. For Windows, *shared resource* refers to any resource that is made available to network users, such as folders, files, printers, and named pipes. *Shared resource* can also refer to a resource on a server that is available to network users. See also server.

**Simple Mail Transfer Protocol (SMTP)** A TCP/IP protocol for sending messages from one computer to another on a network. This protocol is used on the Internet to route e-mail.

**Simple Network Management Protocol (SNMP)** The network management protocol of TCP/IP. In SNMP, agents or clients monitor the activity of various devices on the network and report to the network console workstation. The agents or clients can be hardware as well as software. Control information about each device or service is maintained in a structure known as a management information block. One way to access this information is with Performance Counters. See also Management Information Base (MIB).

**single-threaded apartment (STA)** A form of threading that is supported by Component Object Model (COM). In a single-threaded apartment model, all objects are executed on a single thread and each thread resides within its own apartment.

**SMTP** See definition for Simple Mail Transfer Protocol (SMTP).

**snap-in** A type of tool that you can add to a console supported by Microsoft Management Console (MMC). A stand-alone snap-in can be added by itself; an extension snap-in can be added only to extend the function of another snap-in.

**sniffer** An application or device that can read, monitor, and capture network data exchanges and read network packets. If the packets are not encrypted, a sniffer provides a full view of the data inside the packet. See also packet.

**SNMP** See definition for Simple Network Management Protocol (SNMP).

**socket** An identifier for a particular service on a particular node on a network. The socket consists of a node address and a port number, which identifies the service. For example, port 80 on an Internet node indicates a Web server. There are two kinds of sockets: streams (bidirectional) and datagrams. See also datagram; node.

**SSI** See definition for server-side include (SSI).

**SSL** See definition for Secure Sockets Layer (SSL).

**STA** See definition for single-threaded apartment (STA).

**stateful object** An object that holds private state accumulated from the execution of one or more client calls.

**stateless object** An object that does not hold private state accumulated from the execution of one or more client calls.

**static page** A Hypertext Markup Language (HTML) page that is prepared in advance of a request for it and that is sent to the client upon request. This page takes no special action when it is requested. See also dynamic page.

**structured query language (SQL)** A widely accepted standard database sublanguage used in querying, updating, and managing relational databases.

**subkey** An element of the registry that contains entries or other subkeys. A tier of the registry that is immediately below a key or a subtree (if the subtree has no keys). See also key; registry.

**subnet mask** A 32-bit value that enables the recipient of Internet Protocol version 4 (IPv4) packets to distinguish the network ID and host ID portions of the IPv4 address. Typically, subnet masks use the format 255.*x.x.x*. IPv6 uses network prefix notations rather than subnet masks. See also IP address.

**symmetric encryption** An encryption algorithm that requires the same secret key to be used for both encryption and decryption. Because of its speed, symmetric encryption is typically used when a message sender needs to encrypt large amounts of data. Also called *secret key encryption*. See also public key encryption.

**System Data Source Name (DSN)** A name that can be used by any process on the computer. Internet Information Services (IIS) uses system DSNs to access Open Database Connectivity (ODBC) data sources.

**systemroot** The path and folder name where the Windows system files are located. Typically, this is C:\Windows, although you can designate a different drive or folder when you install Windows. You can use the value %systemroot% to replace the actual location of the folder that contains the Windows system files. To identify your systemroot folder, click **Start**, click **Run**, type **%systemroot%**, and then click **OK**.

**Systems Network Architecture (SNA)** A communications framework developed by IBM to define network functions and establish standards for enabling computers to share and process data.

## T

**T1** A U.S. telephone standard for a transmission facility at digital signal level 1 (DS1) with 1.544 megabits per second in North America and 2.048 megabits per second in Europe. The bit rate is with the equivalent bandwidth of approximately twenty-four 56-kilobits-per-second lines. A T1 circuit is capable of serving a minimum of 48 modems at 28.8 kilobits per second or 96 modems at 14.4 kilobits per second. T1 circuits are also used for voice telephone connections. A single T1 line carries 24 telephone connections with 24 telephone numbers. When it is used for voice transmission, a T1 connection must be split into 24 separate circuits.

**T3** A U.S. telephone standard for a transmission facility at digital signal level 3 (DS3). T3 is equivalent in bandwidth to 28 T1's, and the bit rate is 44.736 megabits per second. T3 is sometimes called a 45-meg circuit.

**TCP/IP** See definition for Transmission Control Protocol/Internet Protocol (TCP/IP).

**Telnet** A protocol that enables an Internet user to log on to and enter commands on a remote computer linked to the Internet, as if the user were using a text-based terminal directly attached to that computer. Telnet is part of the TCP/IP suite of protocols. The term *telnet* also refers to the software (client or server component) that implements this protocol. See also protocol; Transmission Control Protocol/Internet Protocol (TCP/IP).

**thread** A type of object within a process that runs program instructions. Using multiple threads allows concurrent operations within a process and enables one process to run different parts of its program on different processors simultaneously. A thread has its own set of registers, its own kernel stack, a thread environment block, and a user stack in the address space of its process. See also kernel.

**throttling** Controlling the maximum amount of bandwidth that is dedicated to Internet traffic on a server. This feature is useful if there are other services (such as e-mail) sharing the server over a busy link.

**time-out** A setting that automatically cancels an unanswered client request after a certain period of time.

**TP** See definition for transaction processing (TP).

**transaction processing (TP)** The real-time handling of computerized business transactions as they are received by the system. Also called online transaction processing (OLTP).

**Transmission Control Protocol/Internet Protocol (TCP/IP)** A set of networking protocols widely used on the Internet that provides communications across interconnected networks of computers with diverse hardware architectures and various operating systems. TCP/IP includes standards for how computers communicate and conventions for connecting networks and routing traffic. See also Internet Protocol (IP); protocol.

**Transport Layer Security (TLS) encryption** A generic security protocol similar to Secure Sockets Layer (SSL), used with Simple Mail Transfer Protocol (SMTP). See also Secure Sockets Layer (SSL).

**Triple DES (3DES)** An implementation of Data Encryption Standard (DES) encryption that employs three iterations of cryptographic operations on each segment of data. Each iteration uses a 56-bit key for encryption, which yields 168-bit encryption for the data. Although 3DES is slower than DES because of the additional cryptographic calculations, its protection is far stronger than DES. See also cryptography; Data Encryption Standard (DES); encryption.

**two-tier architecture** See definition for client/server architecture.

**type library** A binary file that describes a component's methods, properties, and data structure.

## U

**UNC (Universal Naming Convention) name** The full name of a resource on a network. It conforms to the \\*servername**sharename* syntax, where *servername* is the name of the server and *sharename* is the name of the shared resource. UNC names of directories or files can also include the directory path under the share name, with the following syntax:

\\servername\sharename\directory\filename

**Uniform Resource Locator (URL)** A naming convention that uniquely identifies the location of a computer, directory, or file on the Internet. A URL also specifies the appropriate Internet protocol, such as Hypertext Transfer Protocol (HTTP) or File Transfer Protocol (FTP). An example of a URL is http://www.microsoft.com.

Universal Naming Convention (UNC) A convention for naming files and other resources beginning with two backslashes (\\), indicating that the resource exists on a network computer. UNC names conform to the \\*servername*\*sharename* syntax, where *servername* is the server's name and *sharename* is the name of the shared resource. The UNC name of a directory or file can also include the directory path after the share name, by using the following syntax: \\*servername*\*sharename*\*directory*\*filename*.

upload In communications, the process of transferring a copy of a file from a local computer to a remote computer by means of a modem or network. With a modem-based communications link, the process generally involves instructing the remote computer to prepare to receive the file on its disk and then wait for the transmission to begin.

URL See definition for Uniform Resource Locator (URL).

URL directory See definition for virtual directory.

URL mapping The process of associating a Uniform Resource Locator (URL) with a physical directory. See also virtual directory.

usage data Information that an administrator can use to learn how other people access and use a site. By analyzing this data, an administrator can identify a site's most popular (or unpopular) areas and clarify the most common navigational paths through the site.

user rights Tasks that a user is permitted to perform on a computer system or domain. There are two types of user rights: privileges and logon rights. An example of a privilege is the right to shut down the system. An example of a logon right is the right to log on to a computer locally. Both types are assigned by administrators to individual users or groups as part of the security settings for the computer. See also domain; group.

user type A DWORD that specifies how data is used. A user type is assigned to an identifier in the metabase.

UTF-8 A method of character encoding that allows for both single and multibyte characters in one string. UTF-8 files take up more space than files that are stored in an American National Standards Institute (ANSI) format. Internet Information Services (IIS) supports Web files that are saved in UTF-8 format or in ANSI format. See also code page.

## V

virtual directory A directory name, used in an address, that corresponds to a physical directory on the server. Sometimes called URL mapping.

virtual server A virtual computer that resides on a Hypertext Transfer Protocol (HTTP) server but appears to the user as a separate HTTP server. Several virtual servers can reside on one computer, each capable of running its own programs and each with individualized access to input and peripheral devices. Each virtual server has its own domain name and IP address, and each appears to the user as an individual Web site or File Transfer Protocol (FTP) site. Some Internet service providers (ISPs) use virtual servers for those clients who want to use their own domain names. Also called a Web site.

volatile objects Typically, files that a Web site administrator updates frequently.

## W-Z

W3C See definition for World Wide Web Consortium (W3C).

W3SVC See definition for World Wide Web Publishing Service (WWW service).

WAM See definition for Web Application Manager (WAM).

WBEM See definition for Web-Based Enterprise Management (WBEM).

Web application A software program that uses Hypertext Transfer Protocol (HTTP) for its core communication protocol and that delivers Web-based information to the user in the Hypertext Markup Language (HTML) language. Also called a Web-based application.

Web Application Manager (WAM) For IIS 5.0 isolation mode, a COM+ application package that works with DLLHOST.exe to host out-of-process ISAPI extensions. Provides communication between DLLHOST.exe and INETINFO.exe. See also IIS 5.0 isolation mode.

Web Distributed Authoring and Versioning (WebDAV) An extension to the Hypertext Transfer Protocol (HTTP) 1.1 standard that facilitates access to files and directories through an HTTP connection. Remote authors can add, search, delete, or change directories and documents and their properties.

Web farm A Network Load Balancing cluster of IIS servers that support client Web site requests.

Web garden An application pool served by more than one worker process.

Web page A World Wide Web document. A Web page typically consists of a Hypertext Markup Language (HTML) file, with associated files for graphics and scripts, in a particular directory on a particular computer. It is identified by a Uniform Resource Locator (URL).

Web server In general, a computer that is equipped with server software that uses Internet protocols such as Hypertext Transfer Protocol (HTTP) and File Transfer Protocol (FTP) to respond to Web client requests on a TCP/IP network.

Web service extensions ISAPIs and CGIs that extend Internet Information Services (IIS) functionality beyond serving static pages.

Web-Based Enterprise Management (WBEM) An industry initiative to develop a standard technology for accessing management information about systems in an enterprise environment. The Microsoft implementation of Web-based Enterprise Management is Windows Management Instrumentation (WMI).

WebDAV See definition for Web Distributed Authoring and Versioning (WebDAV).

wide area network (WAN) A communications network connecting geographically separated locations that uses long-distance links of third-party telecommunications vendors. See also local area network (LAN).

wildcard character A keyboard character that can be used to represent one or many characters when conducting a query. The question mark (?) represents a single character, and the asterisk (*) represents one or more characters.

Windows Internet Name Service (WINS) A Windows name resolution service for network basic input/output system (NetBIOS) names. WINS is used by hosts running NetBIOS over TCP/IP (NetBT) to register NetBIOS names and to resolve NetBIOS names to Internet Protocol (IP) addresses. See also IP address.

Windows Management Instrumentation (WMI) The Microsoft implementation of Web-Based Enterprise Management (WBEM), which is an industry-wide standard technology for accessing management information about systems in an enterprise environment. WMI uses the Common Information Model (CIM) industry standard to represent managed components in a system. A system developer can develop a WMI interface that allows programmatic access to a system, so that users can write command-line administration scripts and tools. See also Web-Based Enterprise Management (WBEM).

Windows Script Host (WSH) A language-independent scripting host for ActiveX scripting engines on 32-bit Windows platforms.

WMI See definition for Windows Management Instrumentation (WMI).

WMI provider In Windows Management Instrumentation (WMI), a set of interfaces that provide programmatic access to management information in a system. Internet Information Services (IIS) implements a WMI provider in the namespace called MicrosoftIISv2to provide programmatic access to metabase properties and system settings.

worker process The implementation of the core Web server in Internet Information Services (IIS). Worker processes run in W3wp.exe.

worker process isolation mode The new Web process model for Internet Information Services (IIS) 6.0.

worker thread A thread that is created by a component, Internet Server API (ISAPI) extension, or filter to perform asynchronous processing. Using worker threads frees up Internet Information Services (IIS) I/O threads to process additional requests.

working directory The directory in which Web server software is installed.

working set The RAM that is allocated to a process in the Windows operating system.

World Wide Web (WWW) A set of services that run on top of the Internet and provide a cost-effective way of publishing information, supporting collaboration and workflow, and delivering business applications to connected users all over the world. The Web is a collection of Internet host systems that make these services available on the Internet, using the Hypertext Transfer Protocol (HTTP). Web-based information is usually delivered in the form of hypertext and hypermedia, using Hypertext Markup Language (HTML). The most graphical service on the Internet, the Web also has the most sophisticated linking abilities.

World Wide Web Consortium (W3C) An international industry consortium that is jointly hosted by the Massachusetts Institute of Technology Laboratory for Computer Science (MIT/CS) in North America, by the Institut National de Recherche en Informatique et en Automatique (INRIA) in Europe, and by the Keio University Shonan Fujisawa Campus in Asia. W3C was founded in 1994 to develop common standards for the World Wide Web. Initially, the W3C was established in collaboration with CERN, where the Web originated, with support from the Defense Advanced Research Projects Agency (DARPA) and the European Commission.

World Wide Web Publishing Service (WWW service) The service that manages the Internet Information Services (IIS) core components that process HTTP requests and configure and manage Web applications. Formerly known as W3SVC.

WSH See definition for Windows Script Host (WSH).

WWW See definition for World Wide Web (WWW).

WWW Service Administration and Monitoring component A component of the World Wide Web Publishing Service (WWW service) in Internet Information Services (IIS) that is responsible for configuration, by means of the metabase, and for worker process management.

XML See definition for Extensible Markup Language (XML).